Distr.: Limited
3 April 2018

Original: English

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 3–5 April 2018

Draft report

I. Introduction

1. In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group, to be convened prior to the twentieth session of the Commission, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

2. The first meeting of the Expert Group was held in Vienna from 17 to 21 January 2011. At that meeting, the Expert Group reviewed and adopted a collection of topics and a methodology for the study (E/CN.15/2011/19, annexes I and II).

3. The second meeting of the Expert Group was held from 25 to 28 February 2013. At that meeting, the Expert Group took note of the comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, as prepared by the United Nations Office on Drugs and Crime (UNODC) with the guidance of the Expert Group, pursuant to the mandate contained in General Assembly resolution 65/230 and the collection of topics for consideration within a comprehensive study of the impact of and response to cybercrime and the methodology for that study, as adopted at the first meeting of the Expert Group.

4. In the Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, adopted by the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice and endorsed by the General Assembly in its resolution 70/174, Member States noted the activities of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, and invited the Commission to consider recommending that the Expert Group continue, based on its work, to exchange information on national legislation, best practices, technical assistance and international cooperation, with a

Please recycle

view to examining options to strengthen existing responses and to propose new national and international legal or other responses to cybercrime.

5. The third meeting of the Expert Group was held from 10 to 13 April 2017 At that meeting, the Expert Group considered, inter alia, the adoption of the summaries by the Rapporteur of deliberations at the first and second meetings of the Expert Group, the draft comprehensive study of the problem of cybercrime and comments thereto, and the way forward on the draft study, and exchanged information on national legislation, best practices, technical assistance and international cooperation.

6. In its resolution 26/4, adopted at its twenty-sixth session in May 2017, the Commission on Crime Prevention and Criminal Justice requested the Expert Group to continue its work and, in so doing, to hold periodic meetings and function as the platform for further discussion on substantive issues concerning cybercrime, keeping pace with its evolving trends, and in line with the Salvador Declaration and the Doha Declaration, and requested the Expert Group to continue to exchange information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing responses and propose new national and international legal or other responses to cybercrime.

7. The dates for the fourth meeting of the Expert Group were decided by the extended Bureau by silence procedure on 23 January 2018, and confirmed at its meeting on 26 January 2018.

II. Recommendations

8. During the Expert Group the Rapporteur, with the assistance of the secretariat, noted preliminary suggestions and recommendations focused on strengthening practical responses to cybercrime that were suggested by delegations. A compilation of the suggestions and recommendations is listed as: [...]

III. Summary of deliberations

A. Adoption of the Chair's proposal for the workplan of the Expert Group for the period 2018–2021

9. At its 1st meeting, on 3 April 2018, the Expert Group considered agenda item 1 (c), entitled "Adoption of the Chair's proposal for the workplan of the Expert Group for the period 2018–2021". The Chair's proposal for the workplan of the Expert Group for the period 2018–2021 was adopted.

B. Legislation and frameworks

10. At its [2nd, 3rd and 4th] meetings, on [3 and 4] April 2018, the Expert Group considered agenda item 2, entitled "Legislation and frameworks".

11. The discussion was facilitated by the following panellists: Lu Chuanying (China); George Maria Tyendezwa (Nigeria); Cristina Schulman (Romania); Pedro Verdelho (Portugal); Claudio Peguero (Dominican Republic); Maria Alejandra Daglio (Argentina); and Mohamed Mghari (Morocco).

12. Many delegations referred during the subsequent debate to legislative and policy developments in their countries to address cybercrime and cybersecurity issues. In doing so, they placed emphasis on the key role of capacity-building and technical assistance programmes in supporting successful implementation of national legislation and the building of national capacities for investigations, prosecutions and adjudications, and international cooperation. The need for multidisciplinary approaches involving civil society and the private sector was also highlighted.

13. Many speakers were of the opinion that a new global comprehensive legal instrument on cybercrime was not needed as already existing international instruments such as the Budapest Convention and UNTOC were considered sufficient for developing appropriate domestic and international cooperation responses to cybercrime. In this context, it was highlighted that the Budapest Convention provided an effective legal and operational framework to address cybercrime for both parties to it (including non-members of the Council of Europe) and others for whom the Convention served as a reference, by, inter alia, facilitating international cooperation and harmonization of pertinent criminal law and criminal procedure provisions. Reference was also made to the work of the Cybercrime Convention Committee (T-CY) as well as the capacity-building project GLACY of the Council of Europe, in support of the implementation of the Convention. Next to other outreach projects of technical assistance, for instance within OAS and/or Ecowas. Some speakers also recalled the need to install in any instrument proper conditions and safeguards to protect basic human rights.

14. Other speakers reiterated their opinion that a new legal instrument on cybercrime within the framework of the United Nations is needed. Some speakers stated that they considered the Budapest Convention as a regional legal instrument. Some of the speakers pointed out the closed nature of the accession process of that Convention, namely that it was open for accession by invitation only and subject to the approval of its States parties. Some speakers were of the opinion that the Budapest Convention, in particular its article 32 (b), presented hard to accept challenges in international law such as respect for State sovereignty.

15. As cybercrime was becoming more and more transnational and in many cases are related to organized crime, some speakers considered the United Nations Convention against Transnational Organized Crime relevant to fighting cybercrime.

16. The Expert Group also discussed the relation and differences between cybersecurity and cybercrime; several speakers indicated that the two were different concepts within the very broad challenges of modern use of ICT's. They should therefor be discussed in different and more appropriate forums within the United Nations such as ITU or GGE. Several speakers noted that, however, the topics are interlinked as issues of cybersecurity and needed to be addressed in practice in order to effectively counter cybercrime. A plea was also made for close cooperation and agreements with the private sector.

17. Many speakers expressed appreciation for the work of UNODC through the Global Programme on Cybercrime and shared examples of technical assistance and capacity-building activities carried out under the programme in their countries or regions. Several speakers also noted that other intergovernmental organizations in their regions, such as the Organization of American States and the African Union, were also providing legislative and other types of assistance to counter cybercrime.

18. Speakers expressed appreciation for the work of the Chair and the Bureau of the expert group and of the Secretariat in organizing and preparing for the meeting of the expert group. Many speakers expressed support for the work of the expert group; some speakers stated that it provided a valuable forum for multilateral discussions among experts from diverse jurisdictions. It was further stated that the expert group could play an effective role in discussing responses to the common threats posed by cybercrime, including the technical assistance and capacity-building needs of countries. The adoption by the expert group of the workplan for the period 2018–2021 was welcomed as a step in the right direction.

C. Criminalization

19. At its [4th and 5th] meetings, on [4 and 5] April 2018, the Expert Group considered agenda item, entitled "Criminalization".

IV. Organization of the meeting

A. Opening of the meeting

20. The meeting was opened by André Rypl (Brazil), Vice-President of the Expert Group, in his role as Chair of the fourth meeting of the Expert Group. At the opening of the meeting, statements were made by representatives of [...].

B. Statements

21. Statements were made by experts of the following States: Brazil, China, Ghana, Islamic Republic of Iran, Chile, Ukraine, Ecuador, Argentina, Mexico, Japan, Canada, United States of America, Russian Federation, Colombia, Germany, South Africa, United Kingdom of Great Britain and Northern Ireland, El Salvador, Paraguay, Tunisia, Australia, Costa Rica, Algeria and China.

22. Statements were made by the representative of [...] on behalf of the States Members of the United Nations that are members of the European Union, a regional economic integration organization.

23. Statements were also made by representatives of the following intergovernmental organizations: Council of Europe.

24. Statements were made by representatives of the following academic institutions: [...].

25. Statements were also made by representatives of the following non-governmental organizations: [...].

26. Statements were made by representatives of the following private sector entities: [...].

C. Adoption of the agenda and other organizational matters

27. At its 1st meeting, on 3 April 2018, the Expert Group adopted the following provisional agenda:

1. Organizational matters:
   (a) Opening of the meeting;
   (b) Adoption of the agenda;
   (c) Adoption of the Chair's proposal for the workplan of the Expert Group for the period 2018–2021.
2. Legislation and frameworks.
3. Criminalization.
4. Other matters.
5. Adoption of the report.

D. Attendance

28. The meeting was attended by representatives of 91 Member States, an observer State, a United Nations Secretariat unit, 3 intergovernmental organizations, 9 institutions from the academia and the private sector.

29. A provisional list of participants was circulated at the meeting (UNODC/CCPCJ/EG.4/2018/INF/1).

E. Documentation

30. The Expert Group had before it, in addition to the draft comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, the following documents:

(a) Provisional agenda (UNODC/CCPCJ/EG.4/2018/1);

(b) Chair's Proposal for the 2018–2021 workplan of the Open-ended intergovernmental expert group meeting on Cybercrime, based on Commission on Crime Prevention and Criminal Justice resolution 26/4 (UNODC/CCPCJ/EG.4/2018/CRP.1);

V. Adoption of the report

31. At its 6th meeting, on 5 April 2018, the Expert Group adopted its report (UNODC/CCPCJ/EG.4/2018/L.1).

Distr.: Limited
3 April 2018

Original: English

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 3–5 April 2018

Draft report

Addendum

III. Summary of deliberations

B. Legislation and frameworks (*continued*)

1. During its third meeting, the Expert Group continued its consideration of agenda item 2. Additional points raised by speakers included the importance of ensuring that human rights safeguards in accordance with international law and standards are observed in legislation related to cybercrime and to international cooperation agreements or arrangements, particularly involving electronic evidence. In particular, the importance of balancing the rights to privacy and freedom of expression with the need to prevent and combat cybercrime was discussed. Several speakers stated that they observed a higher degree of convergence of criminalization of cybercrime-related offences in different jurisdictions, which consequently contributed to decreasing fragmentation of legal norms in this field. Remaining challenges reported were the further strengthening of international cooperation efforts, through both formal and informal cooperation practices, and jurisdictional issues raised by cloud computing.

2. The Expert Group further discussed the issue of transborder access to data. It was noted in this regard that deliberations on this matter were very useful in the context of the Expert Group and in other relevant intergovernmental forums, in order to identify best practices and to enhance cooperation among jurisdictions for the investigation of cybercrime. It was further noted that respect of the principle of national sovereignty was an issue that needed to be considered further as it was not always clear how practices in accessing data located in other jurisdictions were compatible with this principle. The proportionality principle in efforts to curb cybercrime was also highlighted. Moreover, many speakers stated that legislation to counter cybercrime needed to use technologically neutral language in order to keep up with the pace of development of technology and crime patterns but should also be specific enough to capture the main criminal activities. Moreover, several speakers highlighted the need to address and respond to the increasing use of the Internet for hate speech, fake news and terrorist purposes, including by creation or updating relevant national legislation. The implementation of any legal framework was perceived to be more effective when accompanied by technical assistance and capacity-building projects.

Please recycle

IV. Organization of the meeting

B. Statements (*continued*)

3. Statements were made by experts of the following States: Algeria, Netherlands, India, Viet Nam, Norway, Jordan, Sri Lanka, China, Turkey, Malaysia, Italy, Serbia, Estonia, Guatemala, Colombia, Mauritius, Kazakhstan, Kuwait, Egypt, Albania, former Yugoslav Republic of Macedonia, Montenegro, Thailand, Bosnia and Herzegovina.

4. Statements were also made by representatives of the following intergovernmental organizations: European Union, Council of Europe, Shanghai Cooperation Council.

V.18-02035

UNODC/CCPCJ/EG.4/2018/L.1/Add.2

Distr.: Limited
4 April 2018

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 3–5 April 2018

Draft report

Addendum

II. Recommendations

Legislation and frameworks (agenda item 2)

1. In line with the Chair's proposal for the 2018–2021 workplan of the Expert Group, adopted by the meeting on its 1st day, at the meetings of the Expert Group in 2018, 2019 and 2020, the Rapporteur, with the necessary assistance of the Secretariat and based on the discussions and deliberations, will prepare a list of preliminary conclusions and recommendations suggested by Member States, which should be precise and focus on strengthening practical responses to cybercrime. Following the workplan, the list is included in the summary report of the meeting as a compilation of suggestions made by Member States, for further discussion at the stock-taking meeting in 2021. As worded in the workplan the Expert Group at the stock-taking meeting will consider the accumulated preliminary conclusions and recommendations in order to produce a consolidated and comprehensive list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

2. Accordingly, the following is the compilation of suggestions made by Member States at the fourth session of the Expert Group in relation to agenda item 2 "Legislation and frameworks":

(a) Member States should, in order for legislative provisions to withstand the test of time with regard to future developments in technology, enact technologically neutral formulated laws that criminalize the activity deemed illegal instead of the means used. Member States should also consider establishing consistent terminology to properly describe the different types of cybercrime activities and facilitate, to the extent possible, accurate interpretation of relevant laws by law enforcement agencies and the judiciary;

(b) Member States should respect the sovereign rights of other States in formulating policies and legislation that meet their national conditions and needs in addressing cybercrime. To foster international cooperation to combat cybercrime, the principle of sovereignty should not be mistakenly interpreted as an obstacle and rather be respected as a fundamental starting point. Volatility of electronic transport and storage of data, such as in so-called clouds, may call for engaging in multilateral

Please recycle

discussions on innovative and expanded mutual assistance between States to ensure timely access to electronic data and evidence;

(c) In order to deny the existence of "safe havens" Member States should offer each other cooperation to the widest extent possible in investigation, evidence collection, prosecution, adjudication and if necessary the removal of illegal content on the Internet. Member States should also provide for the greatest degree of flexibility when providing international cooperation in relation to cybercrimes and other crimes involving electronic data, either as leads in investigations, and, or, as evidence, irrespective of whether the underlying activity is denominated differently in the respective States. In doing so, Member States should bear in mind that dual criminality is usually required for extradition though not necessarily for mutual legal assistance;

(d) Member States should consider, in formulating policies and legislation, the need for striking a balance between human rights protection on the one hand, and national security, public order and legitimate rights of third persons, on the other. National legislations that criminalize conduct and provide for procedural legal authority to permit investigation, prosecution and adjudication of cybercrimes should be consistent with due process guarantees, privacy interests, civil liberties and human rights. National policies and legislations, as well as internationally used and or to be developed instruments should be multidimensional in their approach, on the one hand sharing adequate cybercrime policies from an encompassing understanding of the broader concept of cybersecurity, and on the other hand cover not only illegal behaviour but also focus on prevention of crimes, offering help to individual victims of crime and, or, offer perspectives for the general public to remove from the consequences of cybercrimes. In order to create a solid base for international cooperation on combating cybercrime Member States should strive to find and promote a culture of establishing a common future for cyberspace;

(e) Member States should pursue international cooperation without requiring full harmonization of national legislation as long as the underlying conduct is criminalized, and laws are sufficiently compatible to simplify and expedite the various forms of such cooperation;

(f) Member States should develop, if they have not done so, legislation to provide for extraterritorial jurisdiction over their nationals or ordinary residents to offences irrespective of where the offence occurred and whether the same is regarded as an offence in the foreign jurisdiction;

(g) Member States may draw on different legal bases for international cooperation including reciprocity, as well as bilateral or multilateral treaties and other arrangements. Moreover, Member States with more advanced capacities in the field of cybercrime should assume more responsibilities — proportionate to their capacities or infrastructure — in providing legal assistance to other States;

(h) Member States should consult all relevant stakeholders, including intergovernmental stakeholders, the private sector and civil society, as early as possible when the decision is made to bring forward cybercrime legislation to ensure that relevant issues are properly considered;

(i) Member States should foster strong and trustworthy public-private cooperation in the field of combating cybercrime, including cooperation between government law enforcement authorities and communication service providers (CSPs). Engaging in dialogue with private industry, if possible accompanied by public private partnerships and if needed MOU's is also required to strengthen and facilitate cooperation;

(j) Member States should support UNODC in establishing an educational project/programme focusing on awareness-raising among judicial and prosecution authorities and digital forensic experts of Member States, as well as private entities, about cybercrime and appropriate responses to it; and use capacity-building tools, or

an electronic knowledge management platform to similarly raise awareness of civil society about the impact of cybercrime;

(k) Effective development, enactment and implementation of national legislation to counter cybercrime should be backed up by capacity-building measures and technical assistance programmes. Member States should allocate appropriate resources for domestic capacity-building. The proper implementation of cybercrime-related legislation requires the training of police and prosecutors, as well as public awareness campaigns. Such resources will also further international cooperation as such cooperation is enhanced by country's domestic capacity to investigate and prosecute cybercrime-related offences;

(l) UNODC should engage actively in capacity-building for all Member States in need of assistance, especially developing countries. Such capacity-building activities should be politically neutral and free of condition, result from thorough consultations and be voluntarily accepted by recipient countries. In terms of substance, those capacity-building activities should cover at least the following areas:

(i) Training for judges, prosecutors, investigators and law enforcement authorities in cybercrime investigations, handling of electronic evidence, chain of custody and forensic analysis;

(ii) Drafting and/or amendment as well as implementation of legislation on cybercrime and electronic evidence;

(iii) Structuring cybercrime investigation units and providing guidance on related procedures;

(m) UNODC should seek synergies and cooperate closely with other stakeholders or organizations such as the Council of Europe and the Organization of American States in the field of capacity-building programmes on legislation to ensure that activities and initiatives in this area are not dispersed or fragmented;

(n) Member States should continue using the Expert Group as a platform for exchange of information and best practices, including model laws or model clauses, on such issues as jurisdiction, special investigative techniques, as well as electronic evidence, including challenges posed by its volatile nature and admissibility in court, and international cooperation;

(o) Member States should explore relevant universally accepted practices and rules through multilateral consultation under the auspices of the United Nations and through the Expert Group platform, to avoid fragmentation;

(p) Member States should evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on a regular basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(q) Member States should develop a new international legal instrument on cybercrime within the framework of the United Nations which would take into account the concerns and interests of all Member States;

(r) Member States should use, and, or join existing multilateral legal instruments on cybercrime such as the Budapest Convention as they are evaluated by many States as a best practice model guiding appropriate domestic and international responses to cybercrime;

(s) Existing legal instruments and mechanisms, in particular the United Nations Convention against Transnational Organized Crime should be taken advantage of by as many States as possible to strengthen international cooperation;

(t) Under the auspices of the expert group member States should explore, drawing on best practices in existing regional instruments and/or national legislation, internationally applicable responses, which could be elaborated in the form of model laws or model clauses, where appropriate.

Distr.: Limited
4 April 2018

English only

Expert Group to Conduct a Comprehensive Study on Cybercrime
Vienna, 3-5 April 2018

Draft report

Addendum

II. Recommendations (*continued*)

Criminalization (item 3)

1. In line with the Chair's proposal for the 2018–2021 workplan of the Expert Group, adopted by the meeting on its 1st day, at the meetings of the Expert Group in 2018, 2019 and 2020, the Rapporteur, with the necessary assistance of the Secretariat and based on the discussions and deliberations, will prepare a list of preliminary conclusions and recommendations suggested by Member States, which should be precise and focus on strengthening practical responses to cybercrime. Also according to the workplan, the list will be included in the summary report of the meeting as a compilation of suggestions made by Member States, for further discussion at the stocktaking meeting in 2021. The workplan also states that the Expert Group stocktaking meeting will finish consideration of all the preliminary conclusions and recommendations and will produce a consolidated list of adopted conclusions and recommendations for submission to the Commission on Crime Prevention and Criminal Justice.

2. Accordingly, the following is the compilation of suggestions made by Member States at the fourth session of the Expert Group in relation to agenda item 3 "Criminalization":

(a) Member States should take into account that many substantive criminal law provisions for offline crime can also be applicable for crimes committed online and therefore they should use, for the purpose of strengthening law enforcement, existing provisions in domestic and international law, where appropriate, to tackle those crimes in the online environment;

(b) Member States should adopt and apply domestic legislation to criminalize cybercrime conduct and to provide procedural legal authority to permit law enforcement authorities to investigate alleged crimes consistent with due process guarantees, privacy interests, civil liberties and human rights;

(c) Member States should further pass cyber-specific criminal legislation which takes into account new criminal conduct associated with the misuse of ICTs to avoid relying on generally applicable criminal laws;

Please recycle

(d) Member States should criminalize, taking into account widely recognized international standards, core cybercrime offences that affect the confidentiality, integrity and availability of computer networks and computer data;

(e) Cyber-related acts that are minor infringements rather than of a criminal nature should be addressed by civil and administrative regulations as opposed to criminal legislation;

(f) Member States should consider, if they have not done so, the criminalization of:

- New and emerging forms of cybercrime activities such as the criminal misuse of cryptocurrencies, offences committed on the darknet, the Internet of things, phishing, distribution malwares, and any other software for criminal acts;
- The disclosure of personal information so called "revenge porn";
- The use of Internet for the purpose of terrorism;
- The use of Internet to incite hate crime and violent extremism;
- The provision of technical support or assistance for the perpetration of cybercrime;
- The establishment of illicit online platforms or publishing information for the purpose of perpetrating cyber-related crimes;
- Illegally accessing or hacking into computer systems;
- Illegal interception of, or damage to, computer systems or data;
- Illegal data and system interference;
- Misuse of devices;
- Computer related forgery and fraud;
- Child sexual abuse and exploitation;
- The infringement of copyrights.

(g) Member States should bear in mind that the focus of international harmonization concerning criminalization of cybercrime should be on a core set of offences against the confidentiality, integrity and accessibility of information systems, while a need to harmonize criminalization concerning general offences that are committed using information and communication technology should mainly be dealt with in specialized forums concerning specific areas of crime;

(h) Member States should avoid criminalizing a broad range of activities by Internet service providers, especially where such regulations may improperly limit legitimate speech and expression of ideas and beliefs. Member States should instead work with Internet service providers and the private sector to strengthen cooperation with law enforcement authorities, noting in particular that most Internet service providers have a vested interest in ensuring that their platforms are not abused by criminal actors;

(i) Member States should adopt and implement a domestic legal evidence framework to permit the admission of electronic evidence in criminal investigations and prosecutions, including appropriate sharing of electronic evidence with foreign law enforcement partners;

(j) Member States should use the United Nations Convention against Transnational Organized Crime (UNTOC) to facilitate information and evidence sharing for such criminal investigations, given the frequent involvement of organized crime groups in cybercrime;

(k) Member States should explore ways to help ensure that the exchange of information among investigators and prosecutors dealing with cybercrime is made in

a timely and secure way, including by strengthening networks of national institutions that may be available 24/7;

(l) On the issue of criminalizing ISP's non-compliance with law enforcement, Member States should pay meticulous caution to the detrimental effects on private sector activities and fundamental human rights, in particular, freedom of speech;

(m) In addressing effectively cybercrime, Member States should take into consideration existing human rights frameworks, in particular as regards freedom of expression and the right to privacy; and should further uphold the principles of legality, necessity and proportionality, in criminal proceedings relating to the fight against cybercrime;

(n) Member States should identify trends in the underlying activities of cybercrime through research and further evaluate the possibility and feasibility of mandating the Expert Group or UNODC to conduct and make available on an annual basis, with substantive contributions by Member States, an assessment of cybercrime trends;

(o) Member States should consider the adoption of comprehensive strategies against cybercrime, aimed at developing victimization surveys as well as informing and empowering potential victims of cybercrime. Member States should also consider taking further preventive measures against cybercrime including measures for the responsible use of Internet, especially by children and young people.

III. Summary of deliberations (*continued*)

C. Criminalization

3. At its 4th and 5th meetings, on 4 and 5 April 2018, the Expert Group considered agenda item, entitled "Criminalization".

4. The discussion was facilitated by the following panellists: Malini Govender (South Africa), Li Jingjing (China), Vadim Sushik (Russian Federation), Eric do Val Lacerda Sogocio (Brazil), Marouane Hejjouji (Morocco) and Norman Wong (Canada).

5. Many speakers provided information on the ways in which cybercrime was criminalized in their countries. The most common offences mentioned by speakers included cyber-specific offences, often referred to as "core" cybercrime offences, such as those targeting the confidentiality, integrity and accessibility of computer systems as well as cyber-enabled offences, including offences related to child abuse and exploitation, privacy-related offences, personal data-related offences, the use of the Internet for terrorist purposes, among others. Speakers noted that most countries have legislation already in place to criminalize the core cybercrime offences. It was noted by speakers that it was not necessary for States to have the same crime typology as long as the underlying conducts constituted offences in all jurisdictions, in order to comply with the principle of dual criminality and to eliminate safe havens for criminals.

6. Speakers also emphasized that legislation on the admission of electronic evidence in criminal investigations and prosecutions was needed in order to effectively counter cybercrime, which should be accompanied by adequate training and capacity-building for law enforcement, prosecutors and judges. The importance of sharing of electronic evidence among jurisdictions was also underscored.

7. Speakers shared the experience of their countries in devising legislation and laws to criminalize cybercrime activities. In this regard, experts shared when it was necessary to create new, specific legislation to criminalize certain acts, and when previously-existing legislation and general offences were adequate and sufficient to criminalize new and emerging forms of cybercrime. Many speakers expressed that it was very useful for legislation to be technology-neutral in order to remain applicable in the face of evolving forms of ICTs and cybercrime. It was also noted that each

country had different needs and could consider whether they needed to create new offences depending on the crime trends they faced. Speakers also noted the necessity of having adequate legislation to criminalize new and emerging forms of crime, such as the criminal misuse of cryptocurrency, the internet of things and the dark net, among others.

8. It was also noted that, at the same time, it was important to take into account human rights safeguards when requiring compliance from Internet service providers (ISPs). The Expert Group also discussed types of sanctions for ISPs who failed to cooperate with law enforcement as well as the ways in which the private sector could cooperate in with law enforcement.

9. Regarding the prevention of cybercrime, several speakers emphasized the importance of developing awareness-raising campaigns for the general public as well as targeted education programmes for children in order to inform them about the risks of cybercrime and to improve online safety and cybersecurity for the country as a whole. Moreover, it was stressed that tailored training courses and appropriate allocation of resources were needed in order to enhance the capacities of law enforcement to prevent cybercrime activities.

IV. Organization of the meeting

B. Statements (*continued*)

Criminalization (item 3)

10. Statements were made by experts of the following States: Guatemala, Japan, Colombia, Russian Federation, Norway, Canada, United States of America, India, China, Sri Lanka, Islamic Republic of Iran, Costa Rica, Norway, Indonesia, Philippines, Tunisia, Thailand, South Africa, Belarus, Algeria, Brazil, Ghana, Netherlands, Czechia, Ukraine, Germany, Romania, Lichtenstein, Moldova, Mexico, Serbia, Nigeria, Senegal, Japan, Georgia, Portugal.

11. Statements were also made by representatives of the following intergovernmental organizations: Council of Europe, European Union.